

### REMARKS

Claims 1-58 are presented for prosecution. No claim is currently amended. No claim is cancelled.

The present Office Action appears to ignore Applicant's previous arguments regarding the cite prior art. That is, the Office Repeats many of the same rejections without explaining why Applicant's previously argument were not persuasive. Applicants contacted Examiner Ortiz on April 20, 2006, and noted some of the discrepancies between the Office Action assertions and the Office Action's cited support for such assertions. Examiner Ortiz agreed that there did not appear to be sufficient support for some of the Office Action assertions, and requested that Applicant provide a summary of the invention, and re-submit Applicant's previously filed argument.

Before addressing some of the specific novel features of the present invention, it may adventurous broadly describe a problem being addressed by the present invention. Firstly, controlling access to, and manipulation of, files is a critical and technical part of any computer network. File management is at the core of all computer networks and operating systems. Expanding control of file creation, file access, and file manipulation is an expansion of this technical issue. Thus, a technical problem being addressed by the present invention is how to transfer control of multiple files from a central location, i.e. a network administrator, as is the typical case in the art, to a multitude of individual users. That is, the usual hieratical structure found in a typical computer network (wherein a network administrator typically manages individual users' access and manages the creation and administration of user groups) is removed, and individual control of files is transferred to individual users on either a per user basis or a per file basis.

Claim 1 recites the controlled creation and execution of (presentation) files over the internet. Claim 1 further introduces the control of purchase access (in addition to read-only or read/write access, which is traditionally available in the prior art). It is to be emphasized that purchase access is not the same as execution or edit access, since the purchased filed may be a video recording of an

execution of the file that is sent (i.e. mailed by postal service) to the user or may be a copy of the file that is sent (i.e. mailed) to the user. Adding market control to a network file management system is an expansion of the typical file management within an operating system.

Furthermore, claim 2 explains that inter-file access control does not belong (solely) to a system administrator or group manager. Rather, file access control is managed on a user-by-user basis, wherein one individual user may grant access to a specific other user.

Claim 4 introduces additional levels of file manipulation by reciting that among multiple users that have purchase access to a specific file, one user may remove purchase access from another.

Claim 6 further recites additional file security. Selected users may be given access to a group of password-protected files. However, the selected users must still provide the appropriate password to access a file. Claim 7 explains that the assigning of access to the group of password-protected files is a user-specific operation. Consequently, a user may not know that he/she has been individually granted (password) file access by another user. Claim 8 addresses this issue by explaining that the server provides each registered user a list of all files to which he/she has been granted individual access by another user.

Claims 10 and 11 introduce additional levels of security to password accessible files by specifying various levels of password access permissions.

Returning to the issue of introducing purchase control to a file management system, claim 14 recites a technique by which a sales transaction may be implemented without the transfer of credit card information (or any other financial identifier) to the network server. In this case, the cost of any purchase is incremented to a user's next subscription fee.

As explained above, claim 16 recites not only preferred formats for a purchased file, but specifies the form (video or executable data). That is, claim 16 offers as an option of not only a copy of the presentation file, which by definition is executable, but also offers a recording of the execution of the file. This option overcomes several technical issues associated with incompatibility

between presentation software and/or operating systems and/or available equipment (i.e. computer or DVD/VCR player).

Specific recitations of how files may be managed among individual users are also provided. Specifically, claims 24 and 27-29 explain how individuals may assign and remove permissions to other individual users and how to limit the type of permission granted an individual user to an individual file without the intercession from a network administrator.

Claim 25 explains how users given limited access to a specific file may be prevented from granting other individual users access to the same file.

Since no network administrator is used for assigning and removing access permissions, claim 26 explains how at least one user may be placed in charge of individually managing any one file.

Additionally, multiple users may have "owner status" assigned to the same file. Consequently, each "owner status" user has the power to add and remove other users and to edit the file, therefore there exists the opportunity for malicious abuse of one's access. To limit this abuse, claim 32 introduces the concept of "super owner" status to oust any other user with an "owner status". The "super owners" cannot be removed from a group, and this "super owner" status may be self-transferred among individual users, as indicated in claim 33

Thus, the present invention addresses the technical issue of expanding file manipulation/management in a computer network by removing a traditional hierarchical layer (i.e. the network administrator), and permitting file management by individual users. This makes the present invention better suited for internet applications where a network administrator may find it difficult to keep track of the great multitudes of un-related users that may access an internet website for purposes of creating and/or selling/distributing files.

The present invention, as filed, is specifically applied to the network creation, network administration, network distribution, and network sale of individual presentation file.

Claims 1-2 and 4-13 were rejected under 35 U.S.C. §103(a) as being unpatentable over Kouznetsov et al. (U.S. Pub. 2003/013581) in view of Baker et al. (U.S. Pat. 5,678,041), in view of Skinner (U.S. Pub. 2003/0033311) and further in view of Gabai et al. (U.S. Pat. 6,368,177).

Regarding the Kouznetsov reference, in the telephone conference with Examiner Ortiz, Applicants pointed out that the filing date of the present invention (Feb. 7, 2002) predates the filing date of the Kouznetsov reference (July 17, 2003). However, the Kouznetsov reference does claim priority for part of its content from Provisional Application No. 60/349,879, filed on January 17, 2002. A study of this provisional application showed it to be akin to a sale brochure describing only the proposed use of Macromedia Flash® web browser tools for the creation of presentation files. The provisional reference further suggests that presentation files created using Macromedia Flash® web browser tools may be distributed on the internet by placing the created file on public web spaces (i.e. public folders), or alternatively may be kept private maintaining them in personal spaces (i.e. private folders). In either case, the creator of the presentation file is presumably the only owner of the presentation file, and this ownership cannot be transferred. Thus, Applicants assume that the Kouznetsov reference is relevant only to the extent that it suggests that present files may be created using web browser tools.

Regarding claim 1, the Office Action asserts that Baker et al. (page 3, 1<sup>st</sup> paragraph),

"teaches system and method for restricting user access rights on the internet based on rating information stores in a relational database (see abstract), in which he teaches a network server for controlling the user-creation and user-execution access of presentation files over the internet (see abstract)"

Applicants respectfully disagree. Baker et al. do not teach or suggest any system that controls user creation of any resource on the internet. Rather, Baker et al. explain that they provide portal control to prevent access to targeted web pages that may contain objectionable content. Baker et al. explain that prior art methods of preventing user (particularly children) from accidentally accessing

web pages with objectionable content (such as violent or indecent content) rely primarily on a search of key words on a webpage, and if any objectionable word is found, then the web page is blocked (col. 2, lines 42-48). Baker et al. further explain, however, that such an approach cannot screen for objectionable pictures, and explain that some web page creators are aware of this approach and attempt to avoid objectionable words so as to avoid being blocked. Baker et al. thus suggest viewing all possible web-pages on the internet, and assigning a rating to each web page, such as NV for not violent, or MV for mildly violent, and V for violent (col. 4, lines 52-59). Each user of their web service is assigned an access level that determines if they can only access NV web pages, or NV and MV web pages, or if they can access any web-page without restrictions (col. 4, lines 16-42. Of course, this list of web pages cannot be exhaustive, and any web page that has not been rated is blocked arbitrarily unless the user as permission to access any web-page without restrictions.

The point is that Baker et al. do not teach or suggest any restrictions on user-created content, or access to content created by the user. Baker et al. are concerned with providing violent ratings to web-pages already found on the internet. If the teachings of Baker et al. were combined with the those of Kouznetsov, one would assign a violent rating to Kouznetsov's web page, which provides presentation creation tools. At most, Baker et al. would either permit or deny access to Kouznetsov's web page, and if access were denied, then a user would not be able to access Kouznetsov's web page and not be able to create a presentation file using web tools. This would render Kouznetsov's invention inoperable for its intended purpose.

The Office Action also asserts that Baker et al. teach,

"wherein the user-to-presentation file grouping information includes a created-file group associating each respective registered user to presentation files created by the respective registered user (see column 4, lines 22-32)."

As is explained above, Baker et al. do not rate web pages created by oneself, but rather provide violent ratings to web pages already existing on the internet.

Furthermore, Baker et al. do not teach or suggest creating groups based on who created a web page. They rate web pages based on their violent content.

The Office Action also asserts that Skinner teaches,

"a system and method for collaboration of suppliers through shares interactive data resources (see abstract), in which he teaches the network server maintaining a user-database of registered users and a grouping-database of user-presentation-file grouping information (see abstract; figure 1; and paragraphs 22 and 33)".

Applicants are at a loss to identify where Skinner teaches a grouping-database of user-presentation-file grouping information. As was explained in the previous two Office Action responses, Skinner teaches a system of registered users and registered suppliers. Skinner's system accepts search criteria from a user, and based on the submitted search criteria, generates (in real time) a list of suppliers and products that may meet the user's criteria. This presentation is created instantly, not previously created and stored. Indeed, there is no way that Skinner to know ahead of time what items a user may search for and maintain a "grouping-database of user-presentation-file grouping information".

Furthermore, since Skinner is concern with providing a user with a list of available provides based user-submitted search criteria, if the teachings of Skinner were combined with those of Kouznetsov, one would end up with a system wherein a user submits search criteria for presentation-creation tools to Kouznetsov's web page, and is provided with a list of Macromedia Flash® web browser tools. This combination, however, would not result in a grouping-database of user-to-presentation-file grouping information.

Applicants request that the Examiner please refer to the two previously Office Action Responses for a detailed discussion of the Skinner reference.

The Office Action also asserts that Gabai et al. teach,

"teaches a method for using a toy to conduct sales over a network (see abstract), in which he teaches an executable-file group associating each respective registered user to presentation files to which the respective registered has execution access, and a purchasable-file group associating each respective registered user to presentation files to which

the respective registered user has previously been granted purchase access (see column 86, lines 1-7),"

Applicants respectfully point out that Gabai et al. teach rejecting purchase orders for some items based on a user's permissions. That is, a parent may set a user's purchase limits based on, for example, cost of a toy. However, Gabai et al. permit all users to freely view all presentation files (i.e. view all toys available for sale), but restrict which toys a user may purchased based on pre-submitted parameters (i.e. cost limits). The point is that Gabai et al. do not place any execution access on presentation files since all toy presentation files may be freely accessed and viewed.

Claims 3, 14, 18-19 are rejected under U.S.C. § 103(a) as being unpatentable over Kouznetsov and Gabai et al., as applied above, in and further in view of Stone et al (U.S. Pat. 6,829,587). Applicants respectfully point out that Applicants had already explained in the most-previously submitted Office Action that Stone et al. describe a system for facilitating the publishing of advertisements.

The Office Action cites various figures shown in Stone et al., and makes assertions without providing support from the text of Stone et al. Applicants respectfully request that the Specific text excerpts supporting the use of purchase file groups and the assignment between users of such groups be described.

Claims 20-22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Kouznetsov et al. in view of Baker and Skinner, as described above, and further in view of Stone et al. and Bretschneider et al. (U.S. Pat. 6,128,629). The Office Action asserts that Bretschneider et al. teaches automatically providing presentation file updates in a variety of formats, including video cassette "(see figure 1 column 4, lines 17-26). Applicants previously explained the teachings of Bretschneider et al. in the most recently filed previous Office Action Response. In essence, Bretschneider et al. describe a method by which a software provider (such as Microsoft) may provide software updates to users of its software. In essence, Bretschneider et al. describes a system that, when the software application is used, the applications checks the date of its most recent software

update routine. If the date is past a certain time period, it requests permission for executing an automatic software update by downloading updates from the manufacturer over the internet.

Applicants respectfully request that the Examiner explain how these downloadable software updates may read on the video recording of an execution of the software and the transfer of the video recording on video cassette by postal service to a user. Furthermore, Applicants respectfully point out that one of the objectives of the Bretschneider et al. reference is to avoid the postal mailing of software updates (one CD, for example) by providing an automatic software download process. Applicants respectfully put forth that the use of DVD or video cassette recordings, and particularly the delivery of such by postal mail, is directly opposite to the teaching of Bretschneider et al.

Applicants further respectfully point out that Bretschneider et al. teach that the software provider (i.e. Microsoft) is in control of creating and providing software updates, and no other user may remove Microsoft's ownership of its own software updates. Thus, Applicants are at a loss to determine how Bretschneider et al. may suggest "super-owner" and "owner" statuses assigned to specific presentation files for permitting one individual user to grant access permission to another individual user. Furthermore, how can Bretschneider et al. suggest that the super-owner status and owner statuses may be freely exchanged among users, since Bretschneider et al. provides no method by which Microsoft's ownership of its software updates may be removed from it.

Applicants respectfully request that applicants objections filed in the previously submitted Office Action response please be addressed.



In view of the foregoing amendments and remarks, Applicants respectfully request favorable reconsideration of the present application.

Respectfully submitted,



Rosalio Haro

Registration No. 42,633

Please address all correspondence to:

Epson Research and Development, Inc.  
Intellectual Property Department  
150 River Oaks Parkway, Suite 225  
San Jose, CA 95134  
Phone: (408) 952-6000  
Facsimile: (408) 954-9058  
Customer No. 20178

Date: April 24, 2006